Ente Nazionale per l'Aviazione Civile

# AEROPORTO CIVILE DI LAMEZIA TERME (CZ)

LOTTO L1 - Sviluppo aerostazione passeggeri
CUP: H84G22000030009
LOTTO L2 - Interventi per la security e la digitalizzazione
CUP: H86I22000390002
LOTTO L6 - Potenziamento delle reti di sottoservizi e impianti tecnologici
CUP: H84G22000060009

# PROGETTO ESECUTIVO

## LOTTO L2

## IMPIANTI SECURITY E VIDEOSORVEGLIANZA

## Relazione tecnica impianti security e videosorveglianza

| | | |
|---|---|---|
| GRUPPO DI PROGETTAZIONE<br>Raggruppamento Temporaneo di Professionisti | TECHNITAL | ETS Engineering and Technical Services S.p.A. |
| | Direttore Tecnico e Responsabile integrazione prestazioni specialistiche: ing. Filippo Busola<br>Geologia: dott. Emanuele Fresia<br>Progettazione idraulica: ing. Alessandro Cacciatori<br>Project Manager: ing. Emanuela Perina<br>CSP: arch. Elisabeth Foroni | Direttore Tecnico: ing. Giambattista Parietti<br>Progettazione Specialistica Impianti:<br>ing. Marco Bergami<br>p.i. Daniele Togni<br>ing. Enrico Facchinetti |
| AERTEC | VALLE 3.0 | incide |
| Direttore tecnico: ing. Aeronautico Carlos Berenguer López<br>Responsabile sistemi di trasporto:<br>ing. Pedro Tena Calderón | Direttore tecnico: arch. Emanuela Valle<br>Progettazione architettonica:<br>arch. Maria Camilla Valle<br>arch. Leonardo Giovannozzi | Direttore tecnico e progettazione strutturale:<br>ing. Gianluca Vallerini<br>Coordinatore progettazione strutture: ing. Matteo Pagnozzi |

| CODICE ELABORATO | | | | | | | | REVISIONE | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Fase | Lotto | Ambito | Disciplina | Tipo | Numero | Rev | Scala | Id. | Data | Descrizione |
| E | L2 | 00 | SIC | RE | 01 | A | | A | FEBBRAIO 2025 | EMISSIONE |
| | | | | | | | | B | | |
| | | | | | | | | C | | |
| | | | | | | | | D | | |
| NOME FILE: | AI015P-E-L2-00-SIC-RE-01-A.docx | | | | | | | REDAZIONE: | D. Togni | ETS |

| | | |
|---|---|---|
| Visto del Committente: **Società Aeroportuale Calabrese S.p.A.** | | |
| INTERVENTO FACENTE PARTE DEL<br>Contratto Istituzionale di Sviluppo "CIS VOLARE" | IL RESPONSABILE DEL PROCEDIMENTO:<br>ing. Ferdinando Saracco | IL POST HOLDER DI AREA:<br>OPERATIONAL SERVICES MANAGER: Emilio Parrilla<br>PASSENGER EXPERIENCE MANAGER: Sabrina Mileto<br>PH PROGETTAZIONE: Ferdinando Saracco |
| Approvazione **ENAC:** | | |
| | | |

# INDICE

1. PREMESSA ..... 4
1.1. Oggetto del documento ..... 4
1.2. Progettazione degli impianti ..... 4
1.3. Riferimento a documentazione di progetto esistente ..... 4
1.4. Scopo ..... 4
1.5. Classificazione normativa ai fini della protezione contro l'incendio ..... 5
1.5.1. Attività principale ..... 5
1.6. Classificazione ai sensi della normativa elettrica ..... 5
1.6.1. Luoghi marci di TIPO A ..... 5
1.6.2. Luoghi marci di TIPO B ..... 6
1.6.3. Luoghi marci di TIPO C ..... 6
1.6.4. Conclusioni ..... 6
1.6.5. Locali cabina elettrica C3 ..... 7
1.6.6. Ambienti con pericolo di esplosione ..... 7
1.6.7. Riferimento alla direttiva UE 305/2011 (CPR) ..... 7
1.7. Note relative a marchi commerciali ..... 8
1.8. Acronimi ..... 8
2. NORMATIVE DI RIFERIMENTO ..... 9
2.1. Norme di carattere generale ..... 9
2.2. Norme per ambienti di lavoro o assimilabili ..... 10
2.3. Norme per strutture con rischio di incendio e esplosione ..... 10
2.4. Norme impianto cablaggio strutturato ..... 10
2.5. Norme impianti di telecontrollo ed automazione ..... 10
2.6. Norme impianti antifurto e antintrusione ..... 11
2.7. Norme impianti TV.CC e controllo accessi ..... 11
2.8. Norme per il controllo della rumorosità degli impianti ..... 11
2.9. Norme per i campi elettromagnetici generali dagli impianti ..... 12
2.10. Norme per i rifiuti materiale elettrico ..... 12
2.11. Prodotti da costruzione ..... 13
2.12. Qualità dei materiali ..... 13
3. SOTTOSISTEMA SICUREZZA (VIDEOSORVEGLIANZA) ..... 14
3.1. Definizione e obbiettivi ..... 14
3.1.1. Architettura di riferimento ..... 15
3.2. Funzionalità ..... 15
3.2.1. Funzionalità VMS ..... 17
3.2.2. Licenze SW ..... 21
3.3. Interfacce esterne ..... 21
3.4. Caratteristiche delle apparecchiature ..... 21
3.4.1. Server Centrale ..... 21
3.4.2. Allestimento Control Room ..... 22
3.4.3. Telecamere ..... 22
3.4.4. Telecamere: Quantità e Collocazione ..... 23
3.4.5. NVR ..... 23
3.4.6. Analisi Video storage: stima preliminare capacità ..... 24
4. SOTTOSISTEMA VIDEO ANALISI ..... 25
4.1. Definizione e obbiettivi ..... 25

4.2. Funzionalità (algoritmi) ... 25
4.2.1. Interfaccia Utente ... 26
4.3. Interfacce esterne ... 27
4.4. Caratteristiche delle apparecchiature ... 27
4.4.1. Server ... 27
5. SOTTOSISTEMA CONTROLLO ACCESSI ... 28
5.1. Definizione e obbiettivi ... 28
5.2. Funzionalità ... 28
5.3. Interfacce esterne ... 29
5.4. Caratteristiche delle apparecchiature ... 30
5.4.1. IP Access Control Panel ... 30
5.4.2. Lettore di Badge ... 30
5.4.3. Server ... 30
5.4.4. ACS Client ... 31
5.4.5. Stazioni di Enrolment ... 31
6. SISTEMI DI DIGITALIZZAZIONE ... 32
6.1. Self service kiosk ... 32
6.1.1. Definizione e obiettivi ... 32
6.1.2. Funzionalità ... 32
6.1.3. Interfacce esterne ... 32
6.1.4. Caratteristiche delle apparecchiature ... 32
6.2. Varco Pre-Security e Self Boarding ... 33
6.2.1. Caratteristiche del varco Pre-Security e Self Boarding ... 33
6.2.2. Caratteristiche delle apparecchiature ... 34
6.3. A-B-C eGATES ... 34
6.3.1. Descrizione delle apparecchiature ... 34
6.3.2. Caratteristiche delle apparecchiature ... 35
6.3.3. Accesso varchi e sistema anti accodamento ... 35
6.3.4. Sistema per acquisizione dati biometrici ... 35
6.3.5. Interfacce esterne ... 35
6.4. Caratteristiche tecnologiche ed architetturali ... 36
6.4.1. Caratteristiche tecnologiche ed architetturali e di compliance ... 36
6.4.2. Caratteristiche delle apparecchiature ... 36

# 1. PREMESSA

## 1.1. Oggetto del documento

Il presente documento, allegato alla documentazione del Progetto Esecutivo, ha per oggetto la relazione tecnica degli impianti di security e videosorveglianza relativi al nuovo Terminal partenze ed adeguamento Terminal arrivi, nell'ambito dell'intervento di sviluppo dell'aerostazione passeggeri dell'aeroporto di Lamezia Terme (CZ) – LOTTO 2.

## 1.2. Progettazione degli impianti

Il progetto degli impianti speciali in oggetto è regolamentato ai sensi dell'art.5 del Decreto 22 gennaio 2008 n.37 *"Regolamento concernente l'attuazione dell'articolo 11-quaterdecies, comma 13, lettera a) della legge n.248 del 2 dicembre 2005, recante riordino delle disposizioni in materia di attività di installazione degli impianti all'interno degli edifici"* per l'installazione, la trasformazione e l'ampliamento dei seguenti impianti:

- comma 2, lettera e) "… per gli impianti elettronici in genere quando coesistono con impianti elettrici con obbligo di progettazione"

## 1.3. Riferimento a documentazione di progetto esistente

Il presente progetto esecutivo è stato redatto sulla scorta della documentazione di progetto definitivo (PD) redatto da codesto professionista in rev. A nell'aprile 2024 e rimesso in rev. B a Giugno 2024 a seguito di iter di validazione.

Non sono state apportate modifiche sostanziali al progetto fatto salvo l'esecutivizzazione degli elaborati grafici.

Gli impianti elettrici sono stati "adattati" al lay-out aggiornato dei vari ambienti per alcuni dei quali è stato fatto un cambio di destinazione d'uso rispetto al PD.

Si rimanda all'elenco elaborati di progetto esecutivo.

## 1.4. Scopo

La presente Relazione Tecnica descrive i sottosistemi tecnologici da implementare per la Security e la Digitalizzazione dell'Aerostazione Passeggeri di Lamezia Terme.

Il capitolo 0 descrive il sistema di video sorveglianza VMS (Video Management System).

Il capitolo 4 riguarda il sistema di video analisi che ha il compito di identificare automaticamente eventi di allarme dall'analisi dei flussi di immagine gestiti dal VMS.

Il capitolo 5 tratta del sistema di controllo d'accessi. L'applicazione di Control Room (PSIM- Physical Security Information Management) deve integrare dati da altri sottosistemi al fine di fornire una visione olistica dello stato generale dei terminal dell'aerostazione.

Il capitolo 5 riguarda i sistemi di digitalizzazione che comprendono:

- i self service kiosk
- i varchi di accesso pre-security e self boarding

- gli A-B-C e-gates

## 1.5. Classificazione normativa ai fini della protezione contro l'incendio

### *1.5.1. Attività principale*

Con riferimento alla destinazione d'uso della struttura si applica il seguente decreto:

- D.M. del 17 luglio 2014 "Regola tecnica di prevenzione incendi per la progettazione, la costruzione e l'esercizio delle attività di aerostazioni con superficie coperta accessibile al pubblico superiore a 5000 m2" (G.U. n.173 del 28-07-2014)

## 1.6. Classificazione ai sensi della normativa elettrica

Alla luce di quanto sopra è necessario fare riferimento alla Norma CEI 64-8 del 2021 per valutare se nel fabbricato sono presenti o meno luoghi a maggior rischio in caso di incendio (MARCIO).

### *1.6.1. Luoghi marci di TIPO A*

Trattasi di ambienti con elevata densità di affollamento o elevato tempo di sfollamento in caso di incendio o elevato danno ad animali o cose. La seguente tabella riassume le casistiche:

| ***Codice*** | ***Descrizione*** | ***Esempi*** |
|---|---|---|
| BD2 | Luoghi a bassa densità di affollamento e difficoltà di evacuazione | Fabbricati di altezza elevata (grattacieli, torri, ecc.) |
| BD3 | Luoghi ad alta densità di affollamento e facilità di evacuazione | Ambienti aperti al pubblico (teatri, cinema, centri commerciali, ecc.) |
| BD4 | Luoghi ad alta densità di affollamento e difficoltà di evacuazione | Fabbricati di altezza elevata aperti al pubblico (hotel, ospedali, case di riposo, ecc.) |

Si deve inoltre considerare l'eventuale presenza di attività soggette al controllo dei VVF, che possono far rientrare nella classificazione come luoghi marci di tipo A, di seguito riassunte:

| ***Numero attività*** | ***Descrizione*** |
|---|---|
| 41 | Teatri e studi per le riprese cinematografiche e televisive |
| 64 | Centri informatici di elaborazione e/o archiviazione dati con oltre 25 addetti |
| 65 | Locali di spettacolo e di trattenimento in genere, impianti e centri sportivi, palestre, sia a carattere pubblico che privato, con capienza superiore a 100 persone, ovvero di superficie lorda in pianta al chiuso superiore a 200 mq. Sono escluse le manifestazioni temporanee di qualsiasi genere effettuate in locali o luoghi aperti al pubblico |
| 66 | Alberghi, pensioni, motel, villaggi, residenze, studentati, agriturismi, ostelli, rifugi alpini, bed&breakfast, dormitori, case per ferie, con oltre 25 posti letto. |

| | |
|---|---|
| | Strutture turistiche all'aria aperta (campeggi , villaggi turistici, ecc.) con capacità ricettiva superiore a 400 persone |
| 67 | Scuole di ogni ordine, grado e tipo, collegi, accademie con oltre 100 persone presenti. Asili nido con oltre 30 persone presenti |
| 68 | Ospedali e strutture sanitarie, case di riposo per anziani con oltre 25 posti letto.<br>Strutture ambulatoriali di superficie complessiva superiore a 500 mq. |
| 69 | Locali adibiti ad esposizione e/o vendita all'ingrosso o al dettaglio, fiere e quartieri fieristici, con superficie lorda complessiva superiore a 400 mq. Incluso servizi e depositi. Sono escluse le manifestazioni temporanee, di qualsiasi genere, che si effettuano in locali o luoghi aperti al pubblico |
| 71 | Aziende ed uffici con oltre 300 persone presenti |
| 72 | Edifici sottoposti a tutela, aperti al pubblico, destinati a contenere biblioteche ed archivi, musei, gallerie, esposizioni e mostre |
| 73 | Edificio e/o complessi edilizi ad uso terziario e/o industriale caratterizzati da promiscuità strutturale e/o dei sistemi delle vie di esodo e/o impiantistica con presenza di persone superiori a 300 unità, ovvero di superficie complessiva superiore a 5000 mq. Indipendentemente dal numero di attività costituenti |
| 78 | Aerostazioni, stazioni ferroviarie e marittime, con superficie coperta accessibile al pubblico superiore a 5000 mq., metropolitane in tutto o in parte sotterranee |

L'attività presente nel fabbricato è la 78 che rientra nelle tipologie previste e di conseguenza sono presenti luoghi marci di tipo A.

### *1.6.2. Luoghi marci di TIPO B*

Trattasi di ambienti costruiti prevalentemente in materiali combustibili (per es. legno).

Il fabbricato in oggetto non prevede tale tipologia costruttiva e di conseguenza non sono presenti luoghi marci di tipo B.

### *1.6.3. Luoghi marci di TIPO C*

Trattasi di ambienti con presenza di materiale infiammabile o combustibile in lavorazione, convogliamento, manipolazione o deposito. A tale scopo si considera un carico d'incendio specifico di progetto > 450 MJ/mq.

Nel fabbricato in oggetto non sono previsti ambienti con un simile carico d'incendio e di conseguenza non sono presenti luoghi marci di tipo C.

### *1.6.4. Conclusioni*

Poiché sono presenti luoghi marci di tipo A ne consegue che, con riferimento alla norma CEI 64-8, l'edificio si configura come **a maggior rischio in caso di incendio**.

Di conseguenza l'impianto elettrico dovrà rispettare, oltre che le indicazioni generali della Norma CEI 64-8, anche le prescrizioni aggiuntive della Sezione 751 della norma stessa.

Dovranno altresì essere rispettate le prescrizioni aggiuntive della Sezione 701 relativamente agli ambienti con presenza di bagni e docce.

### *1.6.5. Locali cabina elettrica C3*

L'edificio cabina elettrica C3, nel nuovo polo tecnologico, prevede al suo interno locali tecnici senza presenza continuativa di persone. Alla luce di quanto sopra si possono considerare come AMBIENTI ORDINARI.

Di conseguenza l'impianto elettrico dovrà rispettare solo le indicazioni generali della Norma CEI 64-8 e non le prescrizioni aggiuntive relative agli ambienti a maggior rischio in caso di incendio

Per la parte in media tensione si applicano le prescrizioni delle Norme CEI EN 61936-1 (CEI 99-2) "Impianti elettrici con tensione superiore a 1 kV in corrente alternata", Norma CEI EN 50522 (CEI 99-3) "Messa a terra degli impianti elettrici con tensione superiore a 1 kV in corrente alternata" e Guida CEI 99-5 "Guida per l'esecuzione degli impianti di terra delle utenze attive e passive connesse ai sistemi di distribuzione con tensione superiore a 1 kV in c.a."

### *1.6.6. Ambienti con pericolo di esplosione*

Non sono presenti ambienti e/o attività classificabili con pericolo di esplosione.

Per quanto riguarda i locali contenenti batterie per UPS e soccorritori è stata effettuata la verifica preliminare in merito alla concentrazione in aria dell'idrogeno potenzialmente sviluppabile in fase di finale di carica delle batterie al Pb, per verificarne il limite massimo del 4% (limite inferiore di infiammabilità).

La norma di riferimento relativa alla batterie stazionarie è la EN 62485-2 in fase di recepimento da parte del CEI. I calcoli hanno evidenziato che tale rischio non sussiste e di conseguenza i suddetti locali sono da ritenersi senza con pericolo di esplosione.

### *1.6.7. Riferimento alla direttiva UE 305/2011 (CPR)*

Per quanto riguarda il riferimento alla direttiva UE 305/2011, con riferimento all'utilizzo di cavi conformi al Regolamento Prodotti da Costruzione (CPR), nello sviluppo del progetto esecutivo si sono considerati i seguenti livelli di rischio per la struttura:

- ALTO: per gli ambienti accessibili al pubblico
- MEDIO: per le cabine elettriche, le centrali tecnologiche e le aree completamente all'esterno

A tale proposito si sono previste le seguenti classi prestazionali per i cavi elettrici di potenza e segnale:

- ALTO: classe B2ca - s1a, d1, a1
- MEDIO: classe Cca - s1b, d1, a1

L'eccezione riguarda i cavi degli impianti di rilevazione fumi ed allarme incendio (IRAI) e diffusione sonora di emergenza (EVAC), che fanno riferimento alla norma EN50200, per i quali sono previsti cavi di tipo resistenti al fuoco PH30 e PH120 con classe di reazione Cca - s1b, d1, a1.

## 1.7. Note relative a marchi commerciali

Le indicazioni di tipi e marche commerciali indicate nei documenti ed elaborati di progetto sono da intendersi come dichiarazione di caratteristiche tecniche e come tali non sono vincolanti.

Sono state definite tali tipologie al solo scopo di sviluppo dei calcoli di progetto, al fine di garantire il rispetto e la verifica delle prescrizioni tecniche applicabili all'impianto in oggetto.

## 1.8. Acronimi

| RIF. | ACRONIMO | DESCRIZIONE |
|---|---|---|
| **A** | **ACS** | Access Control System |
| | **API** | Application Programming Interface |
| | **AES** | Advanced Encryption Standard |
| **B** | | |
| **C** | **CCTV** | Closed Circuit TV (camera) |
| **D** | **DBMS** | Database Management System |
| **E** | | |
| **G** | **GPU** | Graphics Processing Unit |
| **H** | **HD** | High Definition |
| **M** | **MP** | Mega Pixel |
| **N** | **NVR** | Network Video Recorder |
| **O** | **OSDP** | Open Supervised Device Protocol |
| | **OWASP** | Open Web Application Security Projec |
| | **OODA** | Observe, Orient, Decide, Act |
| **P** | **PoE** | Power over Ethernet |
| | **PSIM** | Physical Security Information Management |
| | **PTZ** | Pan, Tilt, Zoom |
| **S** | **SSO** | Single Sign-On |
| | **SOP** | Standard Operational Procedure |
| **T** | **TLS** | Transport Layer Security |
| **V** | **VMS** | Video Management System |
| | **VA** | Video Analysis |

## 2. NORMATIVE DI RIFERIMENTO

Gli impianti dovranno essere realizzati al fine di ottenere le migliori condizioni d'utilizzo e sicurezza, nel pieno rispetto delle vigenti leggi, normative e disposizioni particolari degli Enti competenti per Zona e Settore Impiantistico, di cui di seguito si riportano le principali:

### 2.1. Norme di carattere generale

- Legge 1 marzo 1968 n.186 Disposizioni concernenti la produzione di materiali, apparecchiature, macchinari, installazioni e impianti elettrici ed elettronici
- Legge 18 ottobre 1977 n.791 Attuazione della Direttiva del Consiglio delle Comunità Europee (CEE), n.72/73, relativa alle garanzie di sicurezza che deve possedere il materiale elettrico destinato ad essere utilizzato entro alcuni limiti di tensione
- Decreto 22 gennaio 2008 n.37 Regolamento concernente l'attuazione dell'articolo 11-quaterdecies, comma 13, lettera a) della legge n.248 del 2 dicembre 2005, recante riordino delle disposizioni in materia di attività di installazione degli impianti all'interno degli edifici
- Norma CEI 0-2 Guida per la definizione della documentazione di progetto degli impianti elettrici
- Norme CEI 64-8/1-2-3-4-5-6-7-8 IV Ed. Impianti elettrici utilizzatori a tensione nominale non superiore a 1000 V in corrente alternata e a 1500 V in corrente continua
- Norma CEI 64-12 Guida per l'esecuzione dell'impianto di terra negli edifici per uso residenziale e terziario
- Norma CEI 64-14 Guida alle verifiche degli impianti elettrici utilizzatori
- Norma CEI 64-50 Edilizia residenziale – Guida per l'integrazione nell'edificio degli impianti elettrici utilizzatori ausiliari e telefonici
- D.M. del 17/7/14 Norme di prevenzione incendi per aerostazioni con superficie coperta accessibile al pubblico superiore a 5000 $m^2$ (G.U. n.173 del 28/7/14)
- Prescrizioni di Autorità Locali, comprese quelle dei Vigili del Fuoco
- prescrizioni ENAC ed ENAV
- Prescrizioni e indicazioni dell'Azienda Distributrice dell'energia elettrica
- Prescrizioni e raccomandazioni delle ASL
- Prescrizioni e raccomandazioni dell'I.S.P.E.S.L.
- Norme e tabelle di unificazione UNEL ed UNI
- Leggi, regolamenti e circolari tecniche che venissero emanate in corso d'opera
- Normative, Leggi, Decreti Ministeriali regionali o comunali

### 2.2. Norme per ambienti di lavoro o assimilabili

- D.Lgs. n° 81 del 9 aprile 2008 Attuazione dell'articolo 1 della Legge 3 agosto 2007 n.123 in materia di tutela della salute e della sicurezza nei luoghi di lavoro

### 2.3. Norme per strutture con rischio di incendio e esplosione

- Norme CEI 64-8/7 Impianti elettrici utilizzatori a tensione nominale non superiore a 1000 V in corrente alternata e a 1500 V in corrente continua. Parte 7: Ambienti ed applicazioni particolari

### 2.4. Norme impianto cablaggio strutturato

- ANSI/TIA/EIA-568-B.1 Commercial Building Telecommunications Cabling Standard Part 1 : General Requirements of May 2001 ( and all Addendum )
- ANSI/TIA/EIA-568-B.2 Commercial Building Telecommunications Cabling Standard Part 2 : Balanced Twisted-Pair Cabling Components of May 2001 (and all Addendum), and TIA/EIA-568-B.2-1 of June 2002 for CAT6
- ANSI/TIA/EIA-568-B.3 Optical Fiber Cabling Components Standard of April 2000 ( and all Addendum )
- ANSI/TIA/EIA-569-A Commercial Building Standard for Telecommunications Pathways and Spaces of February 1998 ( and all Addendum )
- ANSI/TIA/EIA-606-A Administration Standard for Commercial Telecommunications Infrastructure of May 2002
- ANSI/TIA/EIA-607 Commercial Building Grounding and Bonding Requirements for Telecommunications of August 1994
- Norme EN50173-1 Information Technology Generic Cabling Systems of November 2002
- Norme EN 50174-1 Information Technology – Cabling installation of August 2000
- Norme EN 50174-2 Information Technology – Cabling installation of August 2000
- prEN 50174-3 Information Technology – Cabling installation of March 2002
- Norme ISO/IEC 11801 2nd Edition Information Technology – Generic cabling for customer premises September 2002
- ANSI/EIA/TIA 570-A Residential Telecommunications Cabling Standard of September 1999

### 2.5. Norme impianti di telecontrollo ed automazione

- Norma CEI EN 60870 Sistemi ed apparecchiature di telecontrollo
- Norma CEI EN 50090 Sistemi elettronici per la casa e l'edificio
- Norma CEI 205-2 Guida ai sistemi BUS su doppino per l'automazione nella casa e negli edifici, secondo le Norme CEI EN 50090

- Norma CEI 46-136 Guida alle norme per la scelta e la posa dei cavi per impianti di comunicazione
- Norma CEI EN 60073 1997 Principi fondamentali e di sicurezza per le interfacce uomo-macchina, la marcatura e l'identificazione. Principi di codifica per i dispositivi indicatori e per gli attuatori
- Norma CEI EN 60447 1997 Interfaccia uomo-macchina. Principi di manovra
- Norma CEI EN 60947 1997 Apparecchiatura a bassa tensione.
- Norma CEI EN 60204 "Equipaggiamenti elettrici di macchine industriali.
- Norma CEI 65-5 "Compatibilità elettromagnetica per apparati di misura e comando per processi industriali.

## 2.6. Norme impianti antifurto e antintrusione

- Norma CEI 79-2 Impianti antieffrazione, antintrusione, antifurto e antiaggressione. Norme particolari per le apparecchiature
- Norma CEI 79-3 Impianti antieffrazione, antiintrusione, antifurto e antiaggressione. Norme particolari per gli impianti antieffrazione e antiintrusione
- Norma CEI 79-16 Requisiti per apparecchiature e sistemi di rilevazione e segnalazione di allarme intrusione, antifurto e antiaggressione "senza fili" che utilizzano collegamenti in radio frequenza
- Norma CEI EN 50136-1-1 (CEI 79-18) Sistemi di allarme - Sistemi ed apparati di trasmissione allarmi. Parte 1-1: Requisiti generali per sistemi di trasmissione allarmi

## 2.7. Norme impianti TV.CC e controllo accessi

- Norma CEI 79-4 Impianti antieffrazione, antiintrusione, antifurto e antiaggressione. Norme particolari per il controllo degli accessi
- Norma CEI 79-10 Impianti di allarme. Impianti di sorveglianza CCTV da utilizzare nelle applicazioni di sicurezza. Parte 7: guide di applicazione
- Norma CEI EN 50133-1 (CEI 79-14) Sistemi d'allarme - Sistemi di controllo accesso per l'impiego in applicazioni di sicurezza Parte 1: Requisiti dei sistemi
- Norma CEI EN 50132-5 (CEI 79-38) Sistemi di allarme - Sistemi di sorveglianza CCTV. Parte 5: Trasmissione video
- Norme CEI 79-30 Sistemi di allarme. Sistemi di controllo d'accesso per l'impiego in applicazioni di sicurezza

## 2.8. Norme per il controllo della rumorosità degli impianti

- UNI 8199: Acustica – Collaudo acustico degli impianti di climatizzazione e ventilazione – Linee guida contrattuali e modalità di misurazione

- D.P.C.M. 01.03.91: Limiti massimi di esposizione al rumore negli ambienti abitativi e nell'ambiente esterno
- Legge 26.10.95, N.447: Legge quadro sull'inquinamento acustico
- D.M. 16.03.98: Tecniche di rilevamento e misurazione dell'inquinamento acustico
- D.P.C.M. 14.11.97: Determinazione dei valori limite delle sorgenti sonore
- D.P.C.M. 05.12.97: Determinazione dei requisiti acustici passivi degli edifici
- D.Lgs 19.08.2005, N. 194: Attuazione della direttiva 2002/49/CE relativa alla determinazione e alla gestione del rumore ambientale
- Norme igienico sanitarie della Regione Calabria

### 2.9. Norme per i campi elettromagnetici generali dagli impianti

- CEI 211-6 2001-01 "Guida per la misura e per la valutazione dei campi elettrici e magnetici nell´intervallo di frequenza 0 Hz - 10 kHz, con riferimento all´esposizione umana"
- CEI 211-7 2001-01 "Guida per la misura e per la valutazione dei campi elettromagnetici nell´intervallo di frequenza 10 kHz - 300 Ghz, con riferimento all´esposizione umana"
- CEI 211-4 1996-12 "Guida ai metodi di calcolo dei campi elettrici e magnetici generati da linee elettriche"
- CEI 11-60 2000-07 "Portata ali limite termico delle linee elettriche aeree esterne"
- Linee Guida ICNIRP " Linee guida per la limitazione dell´esposizione a campi elettrici e magnetici variabili nel tempo ed a campi elettromagnetici (fino a 300 GHz)"
- Legge quadro 22/02/2001, n. 36, "Legge quadro sulla protezione dalle esposizioni a campi elettrici, magnetici ed elettromagnetici", G.U. 7 marzo 2001, n. 55
- Decreto Legge 23/01/2001, n.5, "Disposizioni urgenti per il differimento di termini in materia di trasmissioni radiotelevisive analogiche e digitali, nonché per il risanamento di impianti radiotelevisivi", G. U. 24 gennaio 2001, n.19
- Linee guida 01/09/1999 attuazione del Decreto Ministeriale 381/1998
- Decreto Ministeriale 10/09/1998, n. 381, "Regolamento recante norme per la determinazione dei tetti di radiofrequenza compatibili con la salute umana", G.U. 3 novembre 1998, n. 257
- Decreto del Presidente del Consiglio dei Ministri 08/07/2003, "Fissazione dei limiti di esposizione, dei valori di attenzione e degli obiettivi di qualità per la protezione della popolazione dalle esposizioni a campi elettrici, magnetici ed elettromagnetici generati a frequenze comprese tra 100 kHz e 300 GHz", G.U. 28 agosto 2003, n. 199

### 2.10. Norme per i rifiuti materiale elettrico

- Direttiva 2002/96/CE del Parlamento Europeo e del Consiglio del 27 gennaio 2003 sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE)

## 2.11. Prodotti da costruzione

- Regolamento CPR (UE 305/2011) relativamente ai cavi elettrici
- Decreto legislativo n.106/2017 "Adeguamento della normativa nazionale alle disposizioni del regolamento UE n.305/2011 che fissa condizioni armonizzate per la commercializzazione dei prodotti da costruzione e che abroga la direttiva 89/106/CE"

## 2.12. Qualità dei materiali

Tutti i materiali e le apparecchiature previsti per la realizzazione degli impianti in oggetto dovranno essere adatti all'ambiente di installazione, rispondenti alle relative norme CEI-UNEL, ove esistano, e muniti di contrassegno CE.

Inoltre tutti i componenti, per i quali ne sia prevista la concessione dovranno essere dotati del Marchio Italiano di Qualità (IMQ) e/o del contrassegno CEI o di altro Marchio e/o Certificazione equivalente.

In ogni caso, è prescrizione tassativa che tutti i materiali e le apparecchiature siano nuovi, di alta qualità, di sicura affidabilità, di Costruttori che assicurino una rapida e completa disponibilità di ricambi ed una efficace assistenza tecnica, e che siano completi di tutti gli elementi accessori necessari per la loro messa in opera e per il corretto funzionamento.

# 3. SOTTOSISTEMA SICUREZZA (VIDEOSORVEGLIANZA)

## 3.1. Definizione e obbiettivi

Il sistema di gestione della Sicurezza dovrà essere una piattaforma PSIM (Physical Security Information Management) ovvero un sistema in grado di gestire applicativi eterogenei e di integrare allarmi e informazioni provenienti da essi. In particolare saranno integrati i dati almeno provenienti dai seguenti sottosistemi:

- Controllo Accessi
- Chioschi biometrici
- Linee di sicurezza

Il sistema PSIM deve integrare nativamente una piattaforma di videosorveglianza e un sistema di video analisi.

*Estratto dalle specifiche di capitolato di gara*

*Al sistema di videosorveglianza aeroportuale viene chiesto di rilevare, riconoscere e segnalare automaticamente eventi anomali (ad esempio, l'accesso a zone non consentite), generati dall'analisi video delle immagini provenienti da un certo numero di telecamere opportunamente distribuite nelle varie aree.*
*La piattaforma VMS deve consentire la generazione automatica di allarmi, in caso di intrusione nelle aree individuate, con la visualizzazione della telecamera interessata.*

Dovrà essere possibile anche la visualizzazione delle immagini, sia live che registrate, con controllo manuale delle singole telecamere.

Lo PSIM dovrà avere le seguenti caratteristiche generali:

- GIS unico integrato per la visualizzazione degli apparti dei sottosistemi sopra elencati e relativa georeferenziazione;
- Interfaccia utente Web-based;
- Correlazione eventi e allarmi provenienti dai sottosistemi;
- Sistema di workflow per la guida dell'operatore alla risoluzione di criticità/eventi;
- Funzionalità per lo scheduling della gestione di allarmi e operatività automatiche;
- Sistema unificato di comunicazione che integri le componenti sopra elencate.

Dovrà inoltre includere un sistema di Video-analisi basato su tecniche di machine learning con moduli di gestione dei flussi video ed algoritmi dedicati. Questo sistema è trattato nella Sezione 4.

La piattaforma software PSIM è la soluzione che deve gestire i processi di Safety&Security nel contesto di un'infrastruttura critica quale un terminal aeroportuale. La soluzione deve basarsi sulla metodologia OODA (Observe, Orient, Decide, Act) e supportare un'ampia gamma di attività di sicurezza proattiva o reattiva, in una visione integrata di sicurezza.

Tale piattaforma dovrà avere la capacità di integrare differenti sottosistemi e di comparare, correlare e

rappresentare le informazioni in maniera coerente, omogenea ed integrata, provenienti da questi sistemi fornendo una logica business di sicurezza al di sopra di essi.

Lo PSIM dovrà garantire:

- Integrazione delle informazioni provenienti da diversi domini fisici;
- Creazione di una visione complessiva per una maggiore consapevolezza delle situazioni;
- Elaborazione e gestione dei dati acquisiti per fornire informazioni arricchite, con l'obiettivo di supportare la prevenzione degli eventi critici e per individuare le tendenze;
- Monitoraggio centralizzato;
- Coordinamento tra i vari attori coinvolti durante le operazioni.

Lo PSIM dovrà prevedere l'acquisizione dati da sorgenti informative eterogenee e diversificate fornendo una visione sintetica della situazione sul campo (Situation Awareness).

#### *3.1.1. Architettura di riferimento*

Lo PSIM dovrà soddisfare le seguenti caratteristiche architetturali:

- La componente server del software dovrà essere installabile su un server fisico o virtualizzato con sistema operativo e DBMS a scelta del fornitore.
- Il software del Client in Control Room dovrà utilizzare tecnologia web compatibile con le versioni più recenti dei principali browser disponibili sul mercato (Mozilla Firefox, Google Chrome, Microsoft Edge, Safari, ecc.).
- Il software dovrà consentire un collegamento sicuro (crittografato) di tipo SSL o similare tra client e server. La generazione e successivo aggiornamento dei certificati è a carico del Committente, che li renderà disponibile al Fornitore prima dell'avvio operativo dei sistemi.
- Il software dovrà presentare un'interfaccia "user friendly" di controllo e configurazione che consenta di accedere al sistema per configurarne monitoraggi, verifiche e controlli.

### 3.2. Funzionalità

Lo PSIM dovrà integrare i seguenti sistemi:

- la piattaforma PSIM dovrà gestire i flussi video live e registrati provenienti dal sistema VMS;
- Sistema di Controllo Accessi. Tramite questa integrazione, il sistema PSIM riceverà i dati dei transiti dai varchi controllati per successive elaborazioni e presentazione ai supervisori di sicurezza;
- Chioschi biometrici (saranno gestiti allarmi ed eventi nonché informazioni di stato dei dispositivi)
- Linee di sicurezza

Lo PSIM dovrà essere realizzato in modo da consentire l'integrazione dei vari sottosistemi in modo facile e scalabile.

Lo PSIM dovrà disporre di un sistema di correlazione integrato in modo da generare eventi e allarmi complessi provenienti da diversi sottosistemi. Si richiede che il sistema sia in grado di gestire sino a 4.000 eventi gestiti al secondo.

Lo PSIM dovrà essere dotato di un modulo di workflow per la gestione degli allarmi.

Lo PSIM dovrà essere dotato di un modulo GIS per la visualizzazione delle risorse gestite sia fisse che mobile sul territorio.

Lo PSIM dovrà essere dotato di un sistema di geo-localizzazione degli operatori dotati di App mobile dedicata.

Lo PSIM dovrà essere installabile in ambiente virtualizzato garantendo il 99% di disponibilità di servizio. Inoltre, dovrà essere garantita la possibilità di interfacciarsi con sistemi esterni in maniera semplice, sfruttando interfacce SOAP o REST.

Lo PSIM dovrà essere predisposto per supportare una App Android per l'utilizzo da parte di operatori in mobilità consentendo almeno le seguenti funzionalità:

- Invio di allarmi;
- Visualizzazione delle telecamere;
- Geo-localizzazione del dispositivo ove la App è installata;
- Gestione coordinata delle azioni con la Control Room.

Lo PSIM dovrà disporre di una interfaccia di presentazione Web realizzata esclusivamente in HTML5. L'interfaccia dello PSIM dovrà essere in grado di visualizzare almeno 32 flussi video per ciascun operatore utilizzando browser di ultima generazione (non è accettabile l'uso di ActiveX o tecnologie similari).

In termini di interfaccia, lo PSIM dovrà supportare:

- Una modalità per gli operatori: tale modalità fornisce all'operatore un quadro sinottico dello stato dell'area controllata, dei dispositivi e dei sensori, e permette di monitorare la situazione, gestire gli allarmi e le risorse sia attraverso una vista GIS sia attraverso una vista grafica rappresentante un'immagine operativa comune (COP, Common Operational Picture) dell'area. La soluzione proposta deve essere di tipo multi-monitor (almeno 3 Display) e deve supportare la funzione di riallocazione dinamica delle finestre.
- Una modalità per l'analisi dei dati registrati: questa modalità supporta il processo di indagine sugli eventi passati attraverso la ricerca e la visualizzazione delle registrazioni riguardo ad azioni, stati logici, segnali dei sensori fisici, processo decisionale applicato. La soluzione proposta deve consentire l'estrazione delle informazioni sia video che le informazioni relative ad eventi, allarmi, cartografia e workflow operativo.
- Una modalità di amministrazione: questa modalità deve permette di configurare il sistema: creare o modificare gli utenti e i relativi profili, gestire le procedure di workflow, gestire la configurazione di sistema, etc.
- Una modalità di reporting: questa modalità deve permettere di visualizzare i report relativi a:
    - allarmi ricevuti dal sistema filtrabili per tipologia di allarme e fonte;

- eventi ricevuti dal sistema filtrabili per tipologia di evento e fonte;
- elenco allarmi gestititi con la possibilità di verificare il workflow operativo implementato nella gestione;
- elenco attività di accesso al sistema;
- statistica gestione allarmi;
- statistica degli eventi ricevuti da sistema;

Inoltre, le funzionalità e le modalità di gestione fornite dalla piattaforma PSIM dovranno essere fruibili tramite SSO (Single Sign On).

Lo PSIM dovrà essere integrabile con Active Directory.

Lo PSIM dovrà permettere la configurazione di differenti profili senza limitazioni e ad un utente potranno essere associati più profili.

Lo PSIM dovrà supportare una funzionalità di tavolo situazionale dove sia possibile con una interfaccia touchscreen di visualizzare la mappa GIS con gli oggetti mobili e fissi geolocalizzati oltre che gli allarmi che vengono ricevuti dal sistema. Tramite l'interfaccia touchscreen si potranno vedere una o più telecamere con finestra flottante.

Lo PSIM dovrà essere conforme con il GDPR - Regolamento 2016/679.

Lo PSIM dovrà implementare una funzionalità di Videowall in grado di gestire fino a 16 display, gestibile tramite postazione operatore da utente abilitato. La configurazione del Videowall dovrà essere effettuabile in modalità dinamica o attivando degli schemi predeterminati. Il Videowall dovrà consentire la visualizzazione di:

- telecamere live;
- immagini registrate;
- pagine web;
- cartografie GIS.

Dovrà essere possibile personalizzare la vista del sistema e le form presentate in funzione dell'utente e dei relativi privilegi ad esso associati. A tal merito, il sistema dovrà permettere la creazione e configurazione di differenti profili senza limitazioni, nonché la possibilità di associare vari profili ad uno stesso utente.

Tale modulo deve permette la gestione e la visualizzazione di flussi video live provenienti dalle telecamere IP, di registrarli e di fruire del playback dei flussi registrati, nonché il download. La registrazione deve poter essere visualizzata simultaneamente da utenti diversi (applicazione multi-client) sulla rete. La piattaforma PSIM deve supportare l'implementazione di uno o più istanze di VMS a cui poter associare varie telecamere a secondo del sito e/o della ripartizione in gruppi.

### *3.2.1. Funzionalità VMS*

Le principali funzioni del modulo VMS devono essere:

- Registrazione: è la funzione principale e consiste nell'archiviazione dei flussi video dalle varie telecamere presenti nel sistema;
- Streaming: il playback di una registrazione viene fatto attraverso uno streaming video;
- Gestione Risorse: permette la gestione dello spazio disco, cancellando i file vecchi o non più utili;
- Amministrazione: ogni sessione di registrazione deve poter essere configurata in termini di qualità e durata;
- Diagnostica: ogni registrazione viene monitorata per fornire informazioni di diagnostica.

Una funzione di ricerca deve consentire di selezionare il flusso desiderato e l'operatore deve poter esaminare tale flusso video sia attraverso una ricerca su allarme sia su ricerca temporale.

Il sistema VMS deve permettere di controllare il movimento delle telecamere PTZ con mouse, tastiera ed eventuale joystick. I comandi joystick devono essere gestiti con un criterio di priorità: nel caso due utenti diversi cerchino di controllare la stessa: la precedenza è determinata dai privilegi dell'utente. Deve essere previsto un singolo joystick per workstation con il quale deve essere possibile controllare tutte le telecamere motorizzate.

Il VMS deve ricevere e gestire i dati generati dalla telecamera, come minimo i seguenti:

- Stream video
- Eventi degli eventuali algoritmi di analisi dei contenuti video a bordo delle telecamere
- Eventi diagnostici
- Metadati relativi al video

Per tutte le telecamere il sistema gestirà la visualizzazione del live streaming, la registrazione dei flussi video e gli eventi.

Il sistema deve supportare almeno lo streaming video sugli standard H.264+mpeg4 e M-jpeg.

Il VMS deve poter visualizzare flussi video identificati mediante un'azione manuale dell'operatore (Drag & Drop) oppure automaticamente in risposta ad un allarme.

Ogni flusso video deve poter essere visto contemporaneamente da più utenti in tempo reale.

Il sistema deve consentire la visualizzazione simultanea di video e metadati in modalità live e registrati.

Il client di visualizzazione deve supportare in ogni finestra diversi layout come 1x1, 2x2, 3x3, 4x4,

5x5 e molti altri scenari specifici composti ad esempio unendo alcune celle della matrice.

Il sistema deve consentire queste funzionalità di gestione delle telecamere:

- Attivare i preset di una telecamera motorizzata
- Visualizzare una telecamera e un gruppo di telecamere sul videowall
- Attivare uno scenario identificato da un nome: lo scenario è un layout di visualizzazione di un gruppo

di telecamere o altro gruppo di risorse attivabile automaticamente in caso di allarme oppure all'avvio del client.

- Supportare la funzionalità video tour: il video tour può essere configurato su un set di telecamere attraverso l'interfaccia di amministrazione. Il tour configura la sequenza delle telecamere, l'orario di visualizzazione, i preset delle telecamere PTZ.

- Attivare/interrompere una registrazione attraverso l'interfaccia di amministrazione.

Su un flusso video registrato, l'utente può aggiungere un segnalibro per ricordare una posizione sulla timeline.

Il sistema deve mettere a disposizione un tool di pianificazione che consenta agli utenti di configurare l'esecuzione automatica delle attività periodiche.

Il sistema VMS deve supportare la funzione di registrazione attraverso apparati NVR (Network Video Recorder) che possono essere collocati a livello centrale o periferico a seconda delle esigenze.

In caso di interruzione delle comunicazioni tra NVR periferici e storage centrale il salvataggio dei filmati è realizzato dagli NVR locali fino ad un periodo massimo configurabile oltre il quale le registrazioni più vecchie devono essere sovrascritte. Quando le comunicazioni sono ristabilite le registrazioni locali vengono copiato sul server centrale.

I parametri di riferimento sono i seguenti:

- Giorni di registrazione: 7 (registrazione continua)

- Risoluzione 2MP o 8 MP

- Frame rate di registrazione 15 fps

- Codec: H.264

In generale tutte le comunicazioni, comprese quelle tra Client e Server, devono essere crittografate con algoritmi open standard quali AES ed utilizzare il protocollo HTTPS. Tutti i filmati estratti dal sistema devono essere crittografati.

**Gestione Allarmi.**

Il sistema è in grado di gestire tutti gli eventi ricevuti e generare gli allarmi in base alle politiche di generazione allarmi. Gli eventi devono essere elaborati dal modulo di correlazione eventi, che permette di generare allarmi secondo le regole configurate.

Gli eventi gestiti dal sistema devono comprendere le seguenti tipologie:

- Risultati di Video Analisi a bordo delle telecamere

- Risultati di Video Analisi a livello centrale

- Contatti digitali delle telecamere

- Contatti I/O digitali di altro tipo

Tutti questi eventi dal campo verranno gestiti e correlati per generare allarmi basati sulle regole

impostate.

La gestione degli allarmi sarà guidata da una serie di SOP (Standard Operation Procedure) che hanno lo scopo di gestire un allarme con una procedura codificata. Il sistema deve essere dotato di un motore di gestione delle procedure (work flow) basato sullo standard BPM.

Deve essere previsto uno strumento per la generazione e la modifica dei workflow in modo da permettere agli operatori di crearli e modificarli, se necessario.

I work flow devono poter essere avviati nei seguenti istanti:

- All'inizio dell'allarme
- Quando un operatore prende in carico l'allarme
- Quando l'allarme è chiuso.

I work flow devono poter essere personalizzati per ogni tipo di allarme e devono poter eseguire una serie di compiti predefiniti, che sono di due tipi:

- Attività manuali: prevedono un'interazione con l'operatore che gestisce l'allarme
- Attività automatiche: sono azioni automatiche eseguite dal sistema.

Questi sono esempi di attività che possono essere eseguite da un workflow:

- Inviare e-mail contenenti un testo configurabile, un'immagine, un video;
- Attivare uscite digitali (su convertitori IP, telecamere...)
- Attivare telecomandi (sbloccare una porta),
- Visualizzare immagini o video su monitor o postazioni operatore

In questo ambito tutte le azioni eseguite dagli utenti devono essere registrate dal sistema e salvate in un'area di auditing dove tali azioni possono essere consultate da operatori dotati dei privilegi necessari.

**Gestione analisi investigativa.**

La soluzione deve consentire la ricerca intelligente di eventi, allarmi, promemoria, dati memorizzati, segnalibri, metadati, oggetti video o altri eventi associati.

Deve essere possibile vedere gli allarmi storici sulla timeline e posizionare il cursore di riproduzione sull'allarme stesso per vedere il video relativo. Deve essere previsto un filtro degli allarmi da visualizzare sulla timeline.

Il sistema deve generare report contenenti i dati degli allarmi e le relative informazioni allegate comprese sezioni di video. I report disponibili devono poter contenere su richiesta le seguenti informazioni:

- Eventi, filtrati per periodo di tempo, tipo, sensore o sistema che lo ha generato, area geografica.
- Allarmi, filtrati per periodo di tempo, tipo, priorità e area geografica.

- Attività utente sugli allarmi, filtrati per periodo di tempo, operatore, tipo di allarme, priorità ed area.
- Accessi utente, filtrati per periodo di tempo, operatore e ruolo.

Il sistema deve generare pagine statistiche relative almeno alle seguenti quantità:

- Numero totale di allarmi
- Numero di allarmi per tipo
- Numero medio di eventi relativi ad un allarme

**Videowall.**

Deve essere possibile inviare flussi CCTV su di un videowall senza necessità di hardware dedicato (soluzione software). Il videowall può essere diviso in varie aree ognuna delle quali dedicata a visualizzare una specifica telecamera selezionata dall'operatore. I video stream possono essere live oppure provenienti dal video storage (modalità Investigativa).

Il layout su videowall deve poter essere creato, salvato, modificato e cancellato.

#### *3.2.2. Licenze SW*

Tutte le licenze d'uso relative al sistema di PSIM e dei relativi moduli software, dovranno essere di tipo permanente e di durata d'uso illimitata e dovranno essere valide ai fini dell'erogazione dei servizi e funzionalità dichiarati per il sistema. Le licenze d'uso devono coprire l'intera configurazione e dimensionamento necessario.

Le forniture di software di base potranno essere realizzate con l'utilizzo di prodotti Open Source, quale scelta strategica per l'ottimizzazione delle risorse economiche e per la creazione di asset durevoli in forza al Committente.

### 3.3. Interfacce esterne

Il sistema PSIM è l'applicazione principale di controllo generale in Control Room e come tale si deve interfacciare ai seguenti sottosistemi:

- Controllo Accessi (ACS)
- Chioschi biometrici
- Linee di sicurezza

Il sistema PSIM deve integrare dati generati da altri sottosistemi per fornire una visione completa dello stato dell'aerostazione.

Nel caso ACS dovranno essere ricevuti gli allarmi provenienti dai varchi e relativi a situazioni non ammesse come badge non valido oppure apertura forzata di porta allarmata. Dovranno essere anche ricevute informazioni diagnostiche come lettori di varco fuori servizio. PSIM potrà inoltre inviare comandi come chiusura o apertura di porte con serratura elettrificata.

### 3.4. Caratteristiche delle apparecchiature

#### *3.4.1. Server Centrale*

Il sistema PSIM necessita di un Server applicativo con il ruolo di Application Server e di un GEO server (per il sistema GIS). I server avranno le seguenti caratteristiche:

| Descrizione | Specifiche |
|---|---|
| Ruolo | Application Server |
| CPU | 48 Core |
| RAM | 48 GB |
| Storage | 768 GB |
| Sistema Operativo | Microsoft Windows Server |
| Virtualizzazione | HYPER-V o VMWARE |

| Descrizione | Specifiche |
|---|---|
| Ruolo | GEO server |
| CPU | 12 Cores |
| RAM | 16 GB |
| Storage | 500 TB |
| Sistema Operativo | Linux Ubuntu 18 o superiore |
| Virtualizzazione | HYPER-V o VMWARE |

### *3.4.2. Allestimento Control Room*

Devono essere previste 4 VMS workstation con le seguenti caratteristiche:

| Descrizione | Specifiche |
|---|---|
| Ruolo | VMS Workstation |
| CPU | Intel i7 o superiore |
| RAM | 16 GB |
| Storage | 1 TB |
| Sistema Operativo | Microsoft Windows 64 bit |
| Monitor | 3 da 26” risoluzione Full HD 1920x1080 |
| Accessori | Joystick per telecamere PTZ |

Ogni workstation deve essere connessa a 3 monitor in quanto l’interfaccia utente deve presentare almeno 3 viste da destinare ad un monitor dedicato. Una vista deve essere dedicata alla gestione di allarmi ed eventi, una vista è dedicata alla mappa dell’aerostazione ed alla visualizzazione di eventi e risorse geo-localizzate, una vista infine contiene la griglia di visualizzazione delle telecamere CCTV.

Deve essere previsto un Videowall 2X2 con 4 display da 55” (una delle 4 workstation avrà il ruolo id gestore del Videowall).

### *3.4.3. Telecamere*

Devono essere previsti due tipi di telecamera: fissa e PTZ.

La telecamera fissa deve essere digitale (IP network camera). Altre caratteristiche:

- Risoluzione: 2 MP HDTV 1080p (Full HD)
- Frame Rate: fino a 60 fps
- Zoom ottico 32x

- Illuminatore IR integrato con raggio di 80 m
- Protezione ambientale IP66
- Temperatura operativa da -40 °C a 60 °C
- Stabilizzatore elettronico dell'immagine
- ingresso audio per video con audio

La telecamera PTZ “dome” deve essere IP ed avere le seguenti caratteristiche:

- Risoluzione 8MP 4k UHD
- Velocità Zoom
- Zoom: 31x ottico, 12x digitale, Totale 372x
- Messa a fuoco laser integrata
- Frame Rate fino a 30 fps
- Video Analytics a bordo: tracking automatico di persone, motion detection, classificazione oggetti
- Protezione ambientale IP66
- Protezione anti-vandalismo IK10
- Temperatura operativa da -5 °C a 50 °C
- SD Card

#### *3.4.4. Telecamere: Quantità e Collocazione*

Si rimanda agli elaborati grafici di progetto.

#### *3.4.5. NVR*

È il modulo che registra i flussi video da diverse sorgenti (telecamere digitali) su rete TCP/IP. Inoltre, gestisce la riproduzione dei video registrati e il loro eventuale download. Le registrazioni possono essere visualizzate simultaneamente da più utenti (più applicazioni client).

La piattaforma può supportare uno o più NVR, distribuiti in rete. Ad ogni NVR possono essere associate diverse telecamere, in modo da condividere uniformemente l'utilizzo della rete.

Una funzione di Ricerca permette di navigare tra i dati registrati sui server NVR precedentemente configurati. L'utente può visualizzare la registrazione interessata sia in caso di allarme sia in modalità di ricerca libera. L'applicazione recupera e visualizza tutti gli allarmi registrati e rende disponibili all'utente tutti i flussi video corrispondenti.

| Descrizione | Specifiche |
|---|---|
| Ruolo | NVR |

| | |
|---|---|
| CPU | 4 Core |
| RAM | 4 GB |
| Storage | 8 GB Escluso video storage |
| Video Storage | 30 TB |
| Sistema Operativo | Linux |
| Virtualizzazione | HYPER-V o VMWARE |

### *3.4.6. Analisi Video storage: stima preliminare capacità*

| | Nome | Modello | Qtà | Tempo di archiviazione | Larghezza di banda | Archiviazione |
|---|---|---|---|---|---|---|
| Piano Terra | FIX EXT | Fissa | 25 | 7 giorni h24 | 43.0 Mbit/s | 3.25 TB |
| Piano Terra | FIX INT_0 | Fissa | 18 | 7 giorni h24 | 70.1 Mbit/s | 5.30 TB |
| Piano Terra | PTZ EXT | PTZ | 12 | 7 giorni h24 | 53.4 Mbit/s | 4.04 TB |
| Piano Terra | PTZ INT_0 | PTZ | 33 | 7 giorni h24 | 346 Mbit/s | 5.11 TB |
| Primo Piano | PTZ INT_1 | PTZ | 21 | 7 giorni h24 | 164 Mbit/s | 12.4 TB |
| | | | **109** | **Totale:** | **676 Mbit/s** | **30.1 TB** |

# 4. SOTTOSISTEMA VIDEO ANALISI

## 4.1. Definizione e obbiettivi

I sistemi di videosorveglianza producono enormi quantità di file video. La maggioranza degli stream video non è mai guardato o rivisto, per mancanza di tempo o risorse. Di conseguenza, eventuali incidenti legati alla sicurezza potrebbero essere persi e comportamenti sospetti non notati in tempo per prevenire incidenti.

La video analisi consiste nel ridurre la grande quantità di informazioni contenute nei video, rendendole più gestibile per sistemi e persone. I sistemi di analisi video processano automaticamente i video stream provenienti dalle telecamere, generando appropriati tag che identificano comportamenti, situazioni o misure fisiche rilevanti per la sicurezza.

L'analisi video consente inoltre all'operatore di utilizzare il sistema di sorveglianza in modo proattivo e ricevere segnalazioni tempestive su situazioni che potrebbero costituire potenziali rischi. Gli algoritmi disponibili vanno dal semplice rilevamento del movimento al rilevamento di manomissioni delle telecamere, il conteggio delle persone e il rilevamento di situazioni e comportamenti umani particolari.

La video analisi ha il compito di rilevare attività sospette e pericolose e di attivare le video registrazioni di interesse per l'operatore, generare allarmi allertando il personale operativo in campo. Questa tecnologia sposta il focus dalla reazione alla prevenzione.

La piattaforma di Video Analisi (VA) deve poter funzionare in modo indipendente dai dispositivi e dall'infrastruttura di rete e deve poter elaborare video stream live oppure registrati.

In particolare la piattaforma VA deve poter essere configurata in modalità online per l'analisi, la registrazione e la generazione di eventi di allarme oppure offline per l'analisi post-evento.

*Estratto dalle specifiche di capitolato di gara*

- *il motion tracking, ovvero la "rilevazione del movimento";*
- *il rilevamento di oggetti abbandonati (funzione antiterrorismo fondamentale per rilevare borse, valigie, contenitori lasciati incustoditi negli spazi del sito aeroportuale);*
- *il rilevamento di oggetti rimossi*
- *la classificazione degli oggetti*
- *il conteggio di persone e veicoli*
- *il rilevamento ostruzione uscite di emergenza o vie di fuga*
- *l'identificazione aree ad alta densità di traffico*
- *la misurazione della densità dei passeggeri*
- *il rilevamento della presenza di persone in aree non permesse*
- *l'identificazione di persone o mezzi che si muovono in direzioni errate*

## 4.2. Funzionalità (algoritmi)

Di seguito viene fornita la lista degli algoritmi che devono essere forniti.

| Nome | Definizione | Obbiettivo | Specifiche |
|---|---|---|---|
| **Overcrowding detection** | Monitoraggio delle aree dove possono manifestarsi situazioni di grande affollamento o situazioni di accodamento dei | Rilevare il superamento di un livello di affollamento predefinito | L'applicazione deve essere in grado di rendere disponibile una heatmap da sovrapporre al video della telecamera allo scopo di evidenziare in |

| Nome | Definizione | Obbiettivo | Specifiche |
|---|---|---|---|
| | passeggeri. | all'interno di una o più aree di interesse | tempo reale il livello di affollamento rilevato |
| **Left/Removed object** | Rilevazione degli oggetti abbandonati e/o rimossi (ad esempio bagagli abbandonati) | Rilevazione di oggetti abbandonati e/o rimossi | Deve poter essere possibile definire sia una o più tipologie di oggetti (secondo la classificazione comunemente introdotta dall'organizzazione Common Objects in Context COCO) da rilevare sia il tempo di permanenza dell'oggetto nella scena in funzione del particolare scenario applicativo sia la distanza (in metri) massima oltre la quale – dopo il tempo indicato- l'oggetto potrà essere ritenuto abbandonato |
| **Loitering** | Rilevamento di persone che permangono all'interno di un'area più a lungo di un tempo specifico. | Rilevamento di permanenza | Deve essere possibile definire il tempo di loitering, l'area di interesse, la rappresentazione cartografica del percorso della persona |
| **People counting** | Rilevazione della stima numerica degli individui presenti all'interno della scena inquadrata o parte di essa | Conteggio numerico di persone | Generazione di un flusso video con sovra-impresso il numero di persone presenti sulla scena; possibilità di definire una soglia massima di persone oltre la quale viene generato un allarme. |
| **Anti-Intrusion** | Analisi per la rilevazione di intrusioni in aree ad accesso riservato e attraversamenti di linee virtuali (ad esempio per la sicurezza perimetrale della proprietà | Rilevamento di intrusione | Deve consentire di definire un numero qualsiasi di linee virtuali, in modo da dare la possibilità di far scattare un allarme solo se una persona attraversa una serie di linee virtuali in sequenza, e non una sola linea. |

#### *4.2.1. Interfaccia Utente*

L'interfaccia utente del sistema di Video Analisi deve essere integrata con il sistema PSIM/VMS.

Ogni flusso video su cui si effettua il processamento VA deve essere mostrato con informazioni sul risultato dell'algoritmo sovrapposte alle immagini originali. Nello specifico:

- Deve essere disegnato un rettangolo intorno all'oggetto riconosciuto (ad esempio bagaglio o persona)
- Deve essere presentata la stima della percentuale di precisione di riconoscimento di ogni oggetto

nella scena

- Deve essere mostrata un'etichetta associata alla classe dell'oggetto riconosciuta (ad esempio persona)
- Nel caso di algoritmi che processano un'area specifica (ad esempio aree vietate) tale area deve essere identificata sull'immagine (virtual fence o area segregata virtuale)
- Se un oggetto entra nella virtual fence deve essere generato un allarme

L'interfaccia utente deve permettere di disegnare interattivamente la virtual fence per ogni CCTV interessata.

## 4.3. Interfacce esterne

Il sistema di Video Analisi (VA) deve essere strettamente integrato con il VMS. VA deve poter ricevere qualsiasi flusso video gestito da VMS dalla cui interfaccia utente deve essere possibile selezionare quali algoritmi associare ai flussi selezionati. VA deve inviare gli allarmi generati da ogni telecamera il cui flusso video è stato processato al sistema PSIM/VMS.

## 4.4. Caratteristiche delle apparecchiature

### *4.4.1. Server*

| Descrizione | Specifiche |
|---|---|
| Ruolo | Video-analisi |
| CPU | 32 Core |
| RAM | 128 GB |
| Storage | 1 TB |
| GPU | 4 X Tesla T4 (80 algoritmi equivalenti) |
| Sistema Operativo | Microsoft Windows Server |
| Virtualizzazione | Deve essere un server fisico |

# 5. SOTTOSISTEMA CONTROLLO ACCESSI

## 5.1. Definizione e obbiettivi

Il sistema di Controllo Accessi (ACS- Access Control System) ha il compito di controllare tutti i punti di accesso per il personale dell'aeroporto. L'accesso dei passeggeri è gestito da altri sistemi ed apparati.

- In generale le aree segregate dell'aerostazione saranno divise in questo modo:
- Area pubblica: nessun controllo necessario
- Area controllata: il sistema ACS è richiesto
- Area ristretta: il sistema ACS è richiesto con sicurezza avanzata
- Area sterile; il sistema ACS è previsto con un ulteriore livello di screening.

L'accesso tra aree con diverso livello di sicurezza deve essere protetto dal sistema ACS.

La circolazione di emergenza tra diverse aree sicure deve essere possibile ma controllata. Le uscite di emergenza verso aree sicure devono essere controllate da ACS e da telecamere CCTV.

In alcuni casi (ad esempio porte di accesso airside) ACS deve fornire allarmi visivi e sonori.

Deve essere garantita l'integrazione tra ACS e PSIM e VMS per poter associare gli allarmi ACS alle rilevanti telecamere CCTV.

Il sistema ACS si struttura su 3 livelli:

- I server centrali dove risiede il database degli operatori autorizzati con i relativi diritti di accesso ed i moduli di interfaccia con il PSIM per lo scambio di allarmi ed eventi.
- I Controller IP periferici (IP Acces, Control Panel) distribuiti presso i varchi d'accesso e connessi via rete Ethernet ai server centrali. Questi Controller sono unità intelligenti dotate di una copia locale del database degli utenti autorizzati.
- I lettori di badge associati ai varchi d'accesso che possono essere di vario tipo: a contatto, contactless, biometrici.

Il fatto che una copia del database dei badge autorizzati risieda nei Controller periferici permette al sistema ACS di continuare a funzionare in assenza di connessione con i server centrali senza alcun degrado prestazionale.

La soluzione ACS deve essere intrinsecamente scalabile mediante aggiunta di componenti come i Controller IP ed i lettori di badge.

Deve essere garantita la fornitura dei badge fisici e della relativa stampante.

La soluzione deve prevedere la registrazione delle presenze.

## 5.2. Funzionalità

Queste sono le principali Funzionalità che deve implementare il sistema ACS:

- Possibilità di stampare i badge su comando da Client
- Autenticazione esterna via interfaccia OpenID Connect
- Il sistema ACS deve avere una console browser-based da cui poter lanciare tutti i client di monitoraggio e controllo in modalità SSO (Single Sign-On)
- Interfaccia di gestione amministrativa per creare e modificare accounts e credenziali.
- La comunicazione Server-Controller deve essere protetta con crittografia TLS 1.2 o superiore.
- Monitoraggio anti-pass-back
- Possibilità di mascherare allarmi per gruppi di varchi d'accesso
- Monitoraggio del contatore di tentativi d'accesso

La soluzione deve prevedere la possibilità di impostare regole di segnalazione ed invio allarmi in caso di rilevazione di eventi specifici, precedentemente identificati (es. segnalazione apertura determinati.

La soluzione deve prevedere la possibilità di creazione di diversi profili utente di accesso ai quali vengono assegnate diverse configurazioni comportamentali e abilitazioni di accesso alle diverse aree. Deve inoltre essere prevista la possibilità di attribuzione di permessi di accesso con soglie di validità preimpostate e differenziabili per tipologia di accesso.

La soluzione deve prevedere la possibilità di stampare i badge fisici e di creare il layout (foto – campi informazioni utente) personalizzato dei badge di accesso per le varie tipologie di utenti.

La soluzione deve garantire la possibilità di comandare, anche automaticamente, la regolamentazione degli accessi in caso di emergenza.

Dal punto di vista dell'interfaccia utente del software di controllo, la soluzione deve consentire che tutti i dispositivi di campo attestati sui varchi controllati (es. tornelli, porte, ecc.) posti nei diversi punti di accesso alle aree controllate siano navigabili e gestibili attraverso una mappa interattiva che permetta di accedere direttamente alla configurazione del dispositivo di campo.

La gestione dell'emergenza prevede la possibilità di rilevazione delle presenze e la stampa agevole ed immediata dell'elenco preciso delle persone presenti all'interno del sito in un determinato momento, differenziandole per categorie.

Dovrà essere possibile accedere ad un database di informazioni storicizzate riguardo ai dati di anagrafica e timbratura. La soluzione deve essere GDPR compliant e dovrà garantire la conformità al Regolamento Europeo 2016/679, in particolare alla direttiva 95/46/CE, e aderenza a tutte le successive integrazioni in tema di protezione dei dati personali trattati dall'applicazione.

La soluzione deve consentire all'utente di generare ed esportare report personalizzati.

### 5.3. Interfacce esterne

La soluzione deve integrarsi in maniera bidirezionale con protocolli aperti verso la piattaforma di security (PSIM).

Le API devono essere progettate e sviluppate in linea con principi di sviluppo sicuro indicati dalle linee guida aziendali e agli standard riconosciuti (ad esempio OWASP per le Web Application). Le

comunicazioni devono essere protette mediante crittografia (Almeno TLS1.2 IPSec) atti a garantire l'integrità e la riservatezza.

## 5.4. Caratteristiche delle apparecchiature

### *5.4.1. IP Access Control Panel*

E' un apparato edge che permette di interfacciare uno o due lettori di badge ad una singola porta o varco. L'apparato deve avere un'interfaccia Ethernet di tipo PoE Power over Ethernet (802.3af /802.3at).

Una volta configurato il Controller deve funzionare anche in assenza di connessione con il server e deve poter controllare un singolo varco di accesso.

Il Controller deve essere dotato di porte in grado di gestire diverse tipologie di lettore di badge compreso:

- Wiegand
- RS485
- OSDP
- Keypads
- LCD e biometria.

Il Controller deve essere dimensionato per poter caricare in memoria un database per 2 lettori, 240000 badge e 50000 eventi di passaggio.

Il controlller deve avere input digitali per monitorare 2 porte e per l'allarme antivandalismo dell'armadio che lo contiene. Inoltre deve avere due output digitali uno dei quali dedicato alla serratura elettrica della porta controllata.

### *5.4.2. Lettore di Badge*

Il lettore deve avere le seguenti caratteristiche:

- Frequenza operativa di trasmissione: 125kHz / 13.56MHz
- 13.56 MHz Compatibilità Credenziali: Seos, iCLASS, MIFARE Classic, MIFARE DESFire EV1/EV2, FeliCa & CEPAS
- 125 kHz Compatibilità Credenziali: HID Proximity, Indala Proximity, AWID Proximity, EM Proximity
- 2.4 GHz (Bluetooth): Seos (HID Mobile Access)
- IP65 (adatto anche per utilizzo in esterno)

### *5.4.3. Server*

Il server deve essere dimensionato per ospitare almeno 3 Macchine Virtuali (VM), di cui un database centrale e un Server di Comunicazione. Di seguito le caratteristiche:

| Descrizione | Specifiche |
|---|---|
| Ruolo | Database Server |
| CPU | 8 Core |
| RAM | 16 GB |
| Storage | 1 TB |
| Sistema Operativo | Microsoft Windows Server |
| Virtualizzazione | HYPER-V o VMWARE |

| Descrizione | Specifiche |
|---|---|
| Ruolo | Communication Server |
| CPU | 4 Core |
| RAM | 8 GB |
| Storage | 500 GB |
| Sistema Operativo | Microsoft Windows Server |
| Virtualizzazione | HYPER-V o VMWARE |

### *5.4.4. ACS Client*

Si tratta di almeno 2 workstation con le seguenti caratteristiche, da collocare in Control Room:

| Descrizione | Specifiche |
|---|---|
| Ruolo | Workstation |
| CPU | Intel |
| RAM | 4 GB |
| Storage | 500 GB |
| Sistema Operativo | Microsoft Windows 64 bit |
| Monitor | Almeno 26”  1920x1080 Full HD |

### *5.4.5. Stazioni di Enrolment*

Si tratta di una workstation finalizzata alla produzione di badge.

Si tratta di una workstation con le caratteristiche descritte per l’ACS Client con in più i seguenti accessori:

- Lettore di badge
- Lettore biometrico
- Webcam per acquisire la foto per il badge
- Stampante di badge.

# 6. SISTEMI DI DIGITALIZZAZIONE

## 6.1. Self service kiosk

### *6.1.1. Definizione e obiettivi*

L'Unione Europea ha deciso d'istituire un nuovo sistema che registri le informazioni di chi entra, chi esce o viene rifiutato all'ingresso dei confini degli stati membri. La regolamentazione EU 2017/2226 ha stabilito l'entrata in vigore a settembre 2022 di un sistema di Entry/Exit (EES) che detta i confini per le future procedure di controllo delle frontiere a tutti i confini dell'area Schengen includendo un emendamento allo "Schengen Border Code (SBC)" (EU2016/399 – EU2017/2225).

I requisiti per l'acquisizione dei dati dei viaggiatori guideranno necessariamente l'uso di chioschi self-service per ridurre la domanda di agenti di frontiera.

### *6.1.2. Funzionalità*

Il Self-Service Kiosk di Reco 3.26 è un apparato, ad ingombro ridotto, dotato di schermo touch screen, lettore passaporto, telecamere varie (di cui una per acquisizione del volto) e scanner per acquisizione delle impronte digitali, che consente di implementare il processo di "pre-enrollment" del passeggero.

Il SSK consente di effettuare la verifica di autenticità del documento, e acquisire i dati dello stesso;

acquisire l'immagine biometrica del volto; qualora il documento di viaggio contenga un'immagine del volto registrata nel supporto di memorizzazione elettronica (chip) e a tale immagine del volto sia possibile avere accesso in termini tecnici, verificare tale immagine comparandola elettronicamente all'immagine del volto del cittadino di paese terzo interessato rilevata sul posto; registrare i dati EES completi (se di nuova acquisizione) o aggiornati (se necessario); re-indirizzare il passeggero, al termine della procedura di pre-enrollment, verso il corretto step successivo (cabina manuale o e-gate).

<u>Le altezze sono studiate per rendere l'utilizzo facile indipendentemente dall'altezza della persona.</u>

### *6.1.3. Interfacce esterne*

Allo scopo di supportare tutti gli step del processo di pre-enrollment ma anche quello di sistemi esterni (es. e-gate), che utilizzano dati raccolti dal sistema oggetto del presente documento, occorre che il sistema stesso implementi dei "servizi" a consumo di terze parti e dei "client" per l'utilizzo di servizi di terze parti:

- Client per Servizi di integrazione MdI: Il processo di pre-enrollment prevede, per alcuni step, l'integrazione con un certo numero di servizi messi a disposizione dal Ministero degli Interni (servizi SIF/NUI), che definiscono l'unica modalità di interrogazione e scambio dati con il sistema centrale EES.

- L'integrazione con i servizi SIF messi a disposizione dal MdI per le verifiche di autenticità del documento di viaggio, basate su catena di certificazione (CSCA e CRL).

- Servizi per Sistemi esterni: interfacce necessarie per realizzare le integrazioni di processo, con le postazioni "e-gate"

### *6.1.4. Caratteristiche delle apparecchiature*

**Sistema di lettura documenti e carte di imbarco**

Il processo implementato al "chiosco di enrollment" prevede anche la scansione:

- del passaporto o della carta di identità nazionale (di seguito "documento di identità");
- della carta di imbarco (cartacea o su mobile/tablet).

Entrambe le scansioni sono affidate allo stesso dispositivo, REGULA 7028, installato sul chiosco ad altezza conforme a criteri ergonomici e che integra: un lettore di documenti elettronici nei formati e tipologie documento ID1, ID2 e ID3, conformi alle raccomandazioni ICAO 9303 – full page – con superficie di scansione in linea con le indicazioni "ICAO TD3 size"; un lettore di barcode 1D/2D per carte di imbarco.

**Sistema acquisizione biometria facciale**

Per quanto riguarda l'acquisizione del volto, il kiosk è dotato di una soluzione in grado di rilevare il viso della persona mediante telecamere di tipo 2D, per l'acquisizione del volto e una, di tipo 3D, per la valutazione di eventuali attacchi di tipo spoof/PAD.

Il dispositivo utilizza, inoltre, un algoritmo proprietario per eseguire i test di conformità ISO/IEC 19794-5 (Full Frontal Format) e per determinare la "qualità dell'immagine facciale" così come descritto nelle linee guida emesse da FRONTEX per i sistemi EES ("Technical Guide for Border Checks on Entry/Exit Systems (EES)" versione 1.0 di 5/2021).

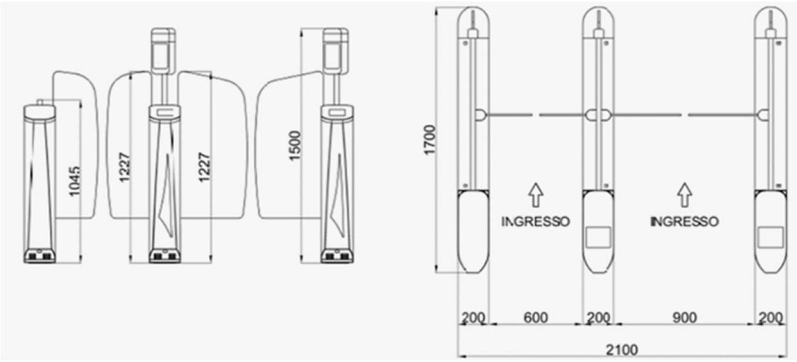
**Sistema acquisizione impronte digitali**

La scansione delle impronte digitali della mano, la relativa valutazione in termini qualità (di quanto acquisito) e la verifica di eventuali attacchi di tipo "spoof"/PAD eventualmente "in corso" (relativamente alle sole impronte digitali), sono affidate, invece, al lettore di impronte digitali, "INTEGRATED BIOMETRICS KOJAK" (e al relativo SDK).

## 6.2. Varco Pre-Security e Self Boarding

### *6.2.1. Caratteristiche del varco Pre-Security e Self Boarding*

Il varco automatico di "pre-security" e "self boarding gestisce i flussi pedonali con o senza bagaglio in ambo le direzioni garantendo un'altissima affidabilità sia in termini di Safety che in termini di Security.




Il varco automatico rispetta la normativa EN16005 in materia di forza di impatto di un ostacolo verso l'utenza

- Al fine di distinguere precisamente l'umano dal bagaglio, quest'ultimo ha un algoritmo specifico;
- I bambini di qualsiasi statura vengono rilevati precisamente dato il posizionamento delle fotocellule;

- Rilevazione accurata di una persona che tenta di transitare in senso opposto;
- Rilevazione accurata di una persona che tenta di passare sopra o sotto gli ostacoli mobili;
- Rilevazione di una "Safety Zone" atta a garantire che gli ostacoli mobili non si aprano/chiudano sull'utente;

Il varco automatico è equipaggiato, in ingresso, di pittogramma di orientamento a LED posizionato verticalmente sul cassonetto destro in modo tale da velocizzare e semplificare il travaso dell'utenza verso la zona controllata.

Il varco è dotato di ventola per il ricircolo dell'aria, di un pulsante per lo sblocco manuale delle ante (dal lato interno) e di un sistema di allarme, audio visivo, per segnalare utilizzi non consentiti (con volume modificabile facilmente anche da operatori della Committente).

#### *6.2.2. Caratteristiche delle apparecchiature*

Sul lato destro del varco, nel rispetto di una disposizione ergonomica e funzionale degli apparati, sono installati:

- uno scanner ottico utilizzato per la lettura di barcodes 2D IATA di ogni tipo, PDF417, EAN13 e decodifica "contactless" di NFC/RFID di smartphone, tablet, smart cards completamente integrato (flat). Risulta posizionato all'estremità di ingresso del varco in posizione idonea alla lettura di carte di imbarco. È prevista una luce led ad evidenziare l'area di lettura del barcode.
- Monitor (per i varchi che prevedono la biometria con il "controllo facciale") dotato di una telecamera ad alta definizione in grado di rilevare i precisi connotati facciali di utenti di altezza compresa tra i 120 ed i 200 cm. La telecamera, grazie alla sua sensoristica unitamente alle sorgenti luminose laterali – integrate – diffuse e adattive (LED), consentono l'acquisizione dell'immagine del volto in diverse condizioni ambientali e di collaborazione del passeggero. L'unità di acquisizione dell'immagine del volto risulta essere dotata di sistema "liveness detection / PAD" di tipo "passivo".
- Alloggiato nel varco vi è un PC con l'applicazione di gestione del varco stesso e del totem biometrico (ove previsto);

### 6.3. A-B-C eGATES

#### *6.3.1. Descrizione delle apparecchiature*

Il sistema proposto mira a migliorare la passenger experience dei passeggeri per i voli extra Schengen, riducendo i tempi d'attesa al controllo passaporti e le operazioni manuali da parte della Polaria. Il sistema proposto è in linea con le normative vigenti in materia di sicurezza e con le linee guida Frontex.

Ad integrazione dei Kiosk EES, l'infrastruttura consta dunque di una soluzione per la gestione di Varchi e-Gates in modalità self-service, integrata con i l'infrastruttura ed i servizi resi disponibili dal Ministero degli Interni, per l'interlocuzione e lo scambio dei dati con il proprio Sistema Centrale.

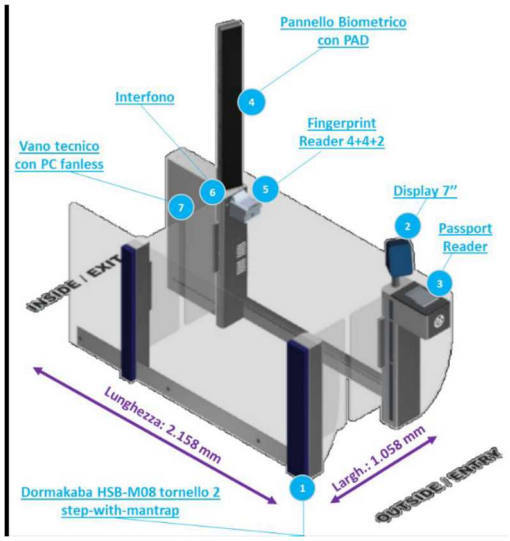
I varchi ABC-Egate sono di tipo "two step with mantrap", conforme alle caratteristiche previste nelle best practice frontex per sistemi ABC ed anche al "Technical Guide Border Checks on Entry/Exit System (EES) equipment".

I Sistemi ABC-Egates , mediante l'impiego di appositi scanner per passaporto e di telecamera per la ripresa del volto del passeggero consentono una verifica diretta anche mediante l'ausilio di rilevazioni biometriche della integrità e della coerenza delle informazioni fornite con quelle presenti nei database

delle Autorità competenti e di Frontiera, favorendo e riducendo le operazioni di controllo.

### *6.3.2. Caratteristiche delle apparecchiature*

Ciascun eGATE ABC è composto dal seguente equipaggiamento:




- Tornello Integrated 2-step with mantrap
- Display integrato disposto sopra lettore Passaporto
- Lettore Documento elettronico
- Pannello di controllo biometrico con telecamera di contesto, telecamera biometrica con specchio digitale, luci contrasto, controllo di vivezza (anti-spoofing) per Presentation Attack Detection (PAD)
- Lettore impronte 4+4+2 con indicatori posizionamento e integrato controllo di vivezza (anti-spoofing – Fake Fingerpint Dectection FFD)
- PC Industriale fanless

Tutte le apparecchiature sopra elencate che compongono il sistema ABC eGates sono soluzioni leader di mercato e tra le più diffuse a livello internazionale e nazionale, nell'ambito di soluzioni di Automated Border Control ed Entry Exit System.

### *6.3.3. Accesso varchi e sistema anti accodamento*

L'accesso ai varchi ABC prevede la lettura del documento elettronico (verifiche sia ottiche sia elettroniche di Passaporto Elettronico e CIE) e in base alle configurazioni relative a età, nazionalità e tipologia documento ammesso verrà o meno aperta la porta di ingresso. In caso di accodamento di passeggeri all'ingresso, il sistema non si limita a segnalare l'accodamento con apposito allarme e mantenendo aperta la porta d'ingresso, ma non appena il secondo passeggero esce automaticamente chiude la porta d'ingresso e procede con la verifica senza dover far uscire anche il primo passeggero e ottimizzando in tal modo il throughput.

### *6.3.4. Sistema per acquisizione dati biometrici*

Una volta entrato nel eGATE e chiusa la porta d'ingresso il sistema utilizza i dati biometrici e visuali raccolti sia per le verifiche con il SIF sia per la verifica con i dati biometrici dell'individuo all'interno del mantrap. La Telecamera biometrica e il lettore impronte digitali 4+4+2 sono entrambe conformi ai requisiti delle Technical Guide Border Checks on Entry/Exit System (EES) equipment oltre a quelli previsti per i sistemi ABC eGates e oltre alla verifica e/o acquisizione dei dati biometrici live sono dotati dei più avanzati sistemi di antispoofing (controllo vivezza).

### *6.3.5. Interfacce esterne*

La soluzione garantisce pienamente l'integrazione funzionale ed interscambio dati con il SIF (Sistema Informativo delle Frontiere) della DCIF, essendo operativa in esercizio fin da luglio 2015, e costantemente aggiornata rispetto le regolamentazioni tecnico/funzionali di settore (es. il sistema ha già disponibile la funzionalità di controllo CIE per i cittadini Italiani.

## 6.4. Caratteristiche tecnologiche ed architetturali

### *6.4.1. Caratteristiche tecnologiche ed architetturali e di compliance*

L'architettura proposta prevede l'utilizzo di una suite di software, librerie e framework, tutti allo stato dell'arte della tecnologia, la cui integrazione persegue e raggiunge l'obiettivo della flessibilità funzionale, affidabilità, scalabilità, condivisione dei servizi.

Relativamente all'Architettura Hardware, viene prevista una configurazione ridondata di tipo "high level", "active active".

### *6.4.2. Caratteristiche delle apparecchiature*

Il sistema progettato per l'ambiente di produzione è strutturato affinché ogni componente software lavori in modalità "Cluster" e/o "Load Balancing" al fine di garantire la massima disponibilità dei dati e dell'infrastruttura. In particolare, la tipologia di High Availability utilizzata è di tipo Active/Active la cui implementazione richiede che l'infrastruttura esegua più istanze delle risorse software formando un cluster, in modo da avere un downtime del servizio pari a zero e una distribuzione del carico di lavoro ottimizzata.

L'architettura consta di:

- 3 server fisici ridondati in HA che ospitano le applicazioni:
  - monitoraggio e controllo
  - gateway per interoperabilità e l'integrazione (sia per la parte EES kiosk che ABC gate)
  - DBMS
- 1 server fisico di management che ospita le applicazioni:
  - monitoraggio dell'infrastruttura
  - gestione dei server virtuali
  - gestione dei backup
- Apparati di rete fisici/virtuali in HA
- 5 postazioni per il controllo manuale dei passaporti dotate di tastiera e monitor (da destinare agli operatori POLARIA)

A supporto, anche l'architettura di rete consta di apparati fisici e virtuali configurati in HA tra di loro, ridondanti anche essi per garantire il servizio.

Per ottimizzare la sicurezza e affidabilità del sistema si prevede l'adozione di appositi software per la gestione del processo di backup e ripristino, elementi fondamentali per arginare incidenti che, altrimenti, potrebbero compromettere il funzionamento di una parte o dell'intera infrastruttura.